The voice of mid-size communications companies

September 30, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: *Ex Parte* Communication: WC Docket No. 16-106

Dear Ms. Dortch:

On September 28, 2016, A.J. Burton of Frontier Communications, Jeb Benedict of CenturyLink, and Genny Morelli and the undersigned of ITTA met with Matthew DelNero, Lisa Hone, and Daniel Kahn of the Wireline Competition Bureau regarding the above-captioned proceeding.[1]

As reflected in the comments filed by ITTA in this proceeding, ITTA continues to maintain that the *NPRM*'s proposals contain significant legal and policy shortcomings.[2] Nevertheless, because Chairman Wheeler appears to continue to be resolute about pushing forward in this proceeding, in the meeting ITTA, while preserving its legal and policy objections,[3] focused its discussion on issues related to consumer consent, data breach notifications, and implementation timelines.

First, ITTA expressed its support for a sensitivity-based approach to consumer consent, along the lines advocated by the Federal Trade Commission and numerous other commenters in this proceeding.[4] Pursuant to this approach, consumer opt-in consent only would be required with respect to use or disclosure of sensitive information, which is composed of financial, health, and children's (through the age of 12) information, Social Security numbers, and precise geolocation information. Moreover, consumers would need to be notified of their right to opt out of the use and disclosure of non-sensitive information, and broadband Internet access service

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) (*NPRM*).

[2] *See* Comments of ITTA, WC Docket No. 16-106 (filed May 27, 2016) (ITTA Comments).

[3] *See id*.; Letter from Michael J. Jacobs, Vice President, Regulatory Affairs, ITTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Aug. 9, 2016).

[4] *See, e.g.*, Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106 (filed May 27, 2016); Letter from Francis M. Buono, Senior Vice President, Legal Regulatory Affairs & Senior Deputy General Counsel, Comcast Corporation, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106 (filed Aug. 1, 2016).

(BIAS) providers would have implied consent to market their products and services to their customers.[5]

Second, ITTA urged that the Commission not adopt additional federal data breach notification requirements for BIAS providers.[6] Forty-seven states, as well as Washington, DC, Guam, Puerto Rico, and the US Virgin Islands have their own data breach notification laws. There is significant commonality among these laws, and even to the extent there are variances, businesses and consumers have successfully navigated these variances for several years. The vast majority of states have a flexible standard for the timing of data breach notifications that takes into account that remedial measures in response to breaches may vary greatly depending on the extent and nature of the particular breach, and they also exclude from notification requirements exposures that do not present a material risk of substantial harm to an individual.[7]

If, nevertheless, the Commission does adopt data breach notification requirements for BIAS providers, it should apply the current CPNI data breach notification rules to BIAS providers.[8] Notifications should only be required for breaches of CPNI or other sensitive

[5] To the extent that such marketing would involve a customer's Customer Proprietary Network Information (CPNI), the Commission has found that authority exists under Section 222(c)(1) of the Communications Act of 1934, as amended, 47 U.S.C. § 222(c)(1), for the Commission to delineate circumstances under which customers have given implied consent to the provider's use of CPNI to market its products and services to its customers, and the Commission has outlined a "total service approach" for when implied consent exists. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8080-81, paras. 23-24 ("We believe that the language of section 222(c)(1)(A) and (B) reflects Congress' judgment that customer approval for carriers to use, disclose, and permit access to CPNI can be inferred in the context of an existing customer carrier relationship. . . . We are persuaded that customers expect that CPNI generated from their entire service will be used by their carrier to market improved service within the parameters of the customer-carrier relationship. . . . [W]ith the likely advent of integrated and bundled service packages, the 'total service approach' accommodates any future changes in customer subscriptions to integrated service."); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended; 2000 Biennial Regulatory Review – Review of Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14866-67, paras. 6-7 ("As service relationships expanded . . . so too did the parameters of the permissible use of CPNI to market new product offerings. This approach recognizes that the customer may be fairly considered to have given implied consent to the carrier's use of CPNI within the total service package to which the customer subscribes. . . . Such sharing was intended to allow carriers with a pre-existing relationship with the customer to develop 'packages' of services best tailored to their customers' needs.").

[6] The Commission could, however, require that it, the Federal Bureau of Investigation, and the United States Secret Service receive notification via "cc:" when a BIAS provider is required to notify appropriate state authorities of a breach under applicable state law.

[7] *See, e.g.,* Arizona Revised Statutes §18-545 (notification must be in the "most expedient manner possible and without unreasonable delay," but is not required, e.g., where the breached information is encrypted or redacted, and the breach does not materially compromise the security or confidentiality of personal information and does not cause and is not reasonably likely to cause substantial economic loss to an individual).

[8] *See* 47 CFR § 64.2011.

information, as discussed above, and the notification requirement should be triggered by the BIAS provider's *determination* of the breach.[9] In addition, the Commission should apply the notification timelines found in the current CPNI rules,[10] including a tolling of the period for notifying consumers if any federal or state law enforcement agency advises the BIAS provider that notification of its customers would impeded a criminal investigation.[11] The Commission should also allow flexibility for entities to combine breach notifications where the breach affects both BIAS and voice customers.

Finally, we advocated for a two-year implementation period for whatever rules the Commission adopts in this proceeding. The implementation burdens on providers promise to be massive, and providers will need to factor these substantial costs into their budget cycles for *next* year and beyond. In addition, mid-size and smaller providers have limited IT resources to engage in the significant web development exercises that will be entailed to properly and accurately notify their customers and other consumers concerning the new privacy requirements. Furthermore, given that the Commission would be adopting a new privacy regime that diverts in numerous facets from the FTC's tried-and-true approach, an extensive consumer education campaign will be entailed to help consumers understand precisely what their rights and responsibilities are under the new regime.

[9] *See id.* § 64.2011(b) (notification requirement triggered "after reasonable determination of the breach"). The notification requirement should not be triggered until, at a minimum, the BIAS provider knows precisely which customers are affected and what customer information was involved in the breach. In the *NPRM*, the Commission proposed that notification requirements be triggered by "discovery" of the breach. 31 FCC Rcd at 2575, para. 234. Regardless of what the Commission intended by "discovery," ITTA urges the Commission, if it adopts new breach notification requirements, to use "determination" as the trigger, both for the sake of consistency with its current CPNI rules as well as overall to avoid confusion. If, nevertheless, the Commission still decides to use the term "discovery," it must clarify what precisely it means by "discovery," and such clarification should encompass the concepts that, at that trigger point, the BIAS provider already has determined the nature and scope of the breach and identified the individuals affected. The absence of such clarification would lead to a notification scheme involving massive over-reporting, and consumers receiving incomplete or inaccurate information, both unnecessarily burdening BIAS providers and creating notice fatigue among consumers.

[10] 47 CFR § 64.2011(b)-(b)(1) (The FBI and Secret Services shall be notified "[a]s soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach," and the carrier "shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification" to the FBI and Secret Service).

[11] *Cf. id.* § 64.2011(b)(3) (tolling of the period for notifying consumers if "the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security").

Please do not hesitate to contact the undersigned with any questions regarding this submission.

Respectfully submitted,

/s/

Michael J. Jacobs
Vice President, Regulatory Affairs

cc: Matthew DelNero
Lisa Hone
Daniel Kahn